

## What is Social Engineering?

Social engineering occurs when an outsider attempts to acquire valuable or sensitive information or inappropriate access privileges. The outsider builds inappropriate or false trust relationships with insiders; acting as a con artist. A social engineer uses both social skills and technical knowledge to fool individuals into believing he or she is trustworthy. The social engineer may seem unassuming and respectable. However, by asking questions, he or she may be able to piece together enough information to infiltrate an agency's networks. If they do not get enough information from one source, they may contact another person within the same agency and rely on the information from the first person to add to his or her credibility.

Social engineers can use human-based methods which rely on person-to-person interactions or computer-based methods which rely on human interaction with computer software, or a combination of the two, to achieve the desired outcome. A common goal is to secretly install spyware or other malicious software that tricks users into revealing passwords or other sensitive information. Examples of social engineering techniques include, impersonation, dumpster diving, phishing, phony web sites, and pop-up windows. This brochure contains helpful, everyday information on how to protect yourself from becoming a victim of social engineers and their tactics.



## Person-to-Person Tactics

### Impersonation

Pretending to be someone in order to gain valuable information; often knows the name and information about that person. Examples of impersonation include: pretending to be a hardware vendor or with Tech Support and requesting password or other access information; OR obtaining the name of someone in the agency who has authority to grant access to information; very effective if person is out of town; OR pretending to be an important person to add an element of intimidation; he or she may threaten to report the user if information is not provided; may pretend to be an unescorted employee or guest dressed in suits or uniforms; looks around for sensitive information

### Dumpster Diving



other discarded materials to find valuable information about the agency or the employees.

Dumpster diving is the practice of looking through an agency's trash for valuable information, either inside or outside the building. Examples include: pretending to be a cleaning person and searching trash receptacles, recycle bins, and

## Computer-Based Tactics

### Phishing

Phishing is the use of email or malicious websites to solicit personal or financial information. This Internet scam prompts a user to provide personal information to a seemingly authentic email. In reality, the email is faked and was created to steal personal information in order to commit fraud. These emails appear to be sent from reputable companies or financial institutions and request the user to provide account information.



The email often indicates that there is a problem with an account or service. When the unsuspecting user responds with the requested information, the attacker then "steals" the personal information or redirects the user to a bogus site in order to gain more information. Any information the user enters is used by the attacker to gain access to the accounts. Phishing emails often contain misspellings, poor grammar, threats, and exaggerations.

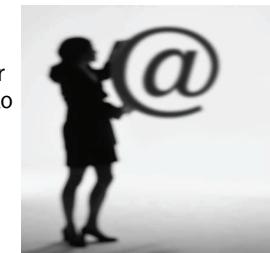
Pharming is often used in with phishing but is not considered social engineering. In this practice, a hacker creates a fake website that copies all the features of the genuine site. Victims may be lured using phishing tactics incorporated in bogus emails. Some users may spot the fake website and avoid being a victim. However, if the attacker hijacks a server, the user will most likely become a victim if the bait is taken.

### Spear Phishing

Spear phishing is also an email attack that is usually targeted toward a particular group of users, most likely in a business environment. Email messages appear genuine to all members within a certain group or agency and seem to be sent by a colleague, employer, or person of authority, such as the head of IT. The emails include requests for user names, passwords, or can contain malicious software.

### Email Attachments

Intruders can hide malicious programs in email attachments. These attachments can spread unwanted files that cause damage to the user's computer and those of others. The attachments usually have "friendly" headings or may appear to be sent from someone known to the user. However, they actually contain viruses, worms, or Trojan horse files. The intruder may use the email as a way to send spam, chain letters, or hoaxes. Chain letters do not usually cause physical damage to the system, network, or information they can cause large losses in productivity and use up valuable network resources.



### Pop-up Windows

Message windows may appear on a user's screen in various formats: a message indicates that network connection has been lost and the user should reenter the user name and password; a program installed earlier by an intruder, will email the user's information to a remote site; an ad entices users about products via the link provided; the user is rerouted to a bogus site in order to reveal valuable information; or an ad offers a contest or free gift, to participate, the user provides email address and password information that the attacker uses to gain network access.



## Avoidance Techniques

Avoid becoming a victim of social engineering scams by following the tips listed here:

- Be suspicious of unsolicited phone calls, visits, or emails asking about employees or other internal information; try to verify the identity of the person directly with the company
- Do not provide passwords, personal or agency information unless you are certain of the person's authority to have the information

- Do not reveal personal, financial, or medical information in emails, and do not respond to email solicitations for this information; do not follow email links
- Do not send sensitive information over the Internet before checking a website's security
- Be wary of what you discard in public receptacles; dispose of valuable, sensitive, or proprietary information in the appropriate manner
- Be suspicious of unexpected emails or emails from unknown persons containing attachments; screen attachments before opening
- Do not click on hyperlinks in emails if you suspect the message is not authentic or the source is unknown
- Notice the URL of a website; malicious sites may look identical to the real site, but the URL may use a variation in spelling or different domain (e.g., .com vs. .net)
- To verify an email, contact the company directly. Do not use contact information provided on the web site
- Install and maintain anti-virus software, firewalls, and email filters; use pop up blockers
- If you think you revealed agency-sensitive information, report it to the appropriate people within your agency, including network administrators
- If you think your accounts were compromised, contact the institution immediately and close any accounts that may have been effected; watch for unexplained charges and report the attack to the police and the Federal Trade Commission (<http://www.ftc.gov>)
- Ensure employees are properly trained, follow security procedures, and exercise caution when using peer-to-peer file sharing

For more information refer to: OnGuard OnLine at <http://www.onguardonline.gov> OR US-CERT at <http://www.us-cert.gov>



U.S. Department of Health and Human Services



U.S. Department of Health and Human Services



### Points of Contact

#### In your OPDIV:

OPDIV Help Desk: \_\_\_\_\_

OPDIV CISO: \_\_\_\_\_

#### Secure One HHS

[SecureOne.hhs@hhs.gov](mailto:SecureOne.hhs@hhs.gov)

<http://intranet.hhs.gov/infosec>

#### Office of Security and Drug Testing (OSDT):

<http://intranet.hhs.gov/osdt>

#### Office of the Inspector General (OIG)\*

OIG Hotline: 1-800-HHS-TIPS

[www.oig.hhs.gov/hotline.html](http://www.oig.hhs.gov/hotline.html)

\*Report suspected fraud or abuse of Departmental programs.

# Quick Guide to Social Engineering Scams



DEPARTMENT OF HEALTH & HUMAN SERVICES - USA

**HHS Security and Privacy Awareness Day**  
**Protecting You and Your Family**